PATENT APPLICATION
DOCKET NO. 0500.0008171

In the United States Patent and Trademark Office

FILING OF A UNITED STATES PATENT APPLICATION

Title:

METHOD AND APPARATUS FOR PROVIDING USER AUTHENTICATION

Inventors:

Ron J. Vandergeest 180 Equestrian Drive Kanata, Ontario, Canada	Kevin T. Simzer 1438 Forge Street Gloucester, Ontario, Canada
Eric Skinner 126 Second Avenue, Apt. #1 Ottawa, Ontario, Canada K1S2H5	

Attorney of Record
Christopher J. Reckamp
Registration No. 34,414
P.O. Box 06229
Wacker Drive
Chicago, IL 60606-0229
Phone (312) 939-9800
Fax (312) 939-9828

Express Mail Label No. EL504284465US

Date of Deposit: 12/22/00

I hereby certify that this paper is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. Section 1.10 on the 'Date of Deposit', indicated above, and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Name of Depositor: Rosalie Swanson
(print or type)

Signature: Rosalie Swanson

PATENT APPLICATION

Attorney Docket No. 0500.0008171

METHOD AND APPARATUS FOR PROVIDING USER AUTHENTICATION

Field Of The Invention

The invention relates generally to methods and apparatus for providing user authentication to allow a user to gain access to an application(s) or system, and more particularly to methods and apparatus for providing user authentication using multi-factor authentication techniques.

Background Of The Invention

Many secure access techniques are known to gain access to secure computer systems, bank accounts, and other processes within a computer or Internet appliance. For example, communication units include Web browsers that may be used to gain access to Web-based information from a Web server and may be coupled via a wireless or non-wireless communication link. Techniques are known to provide per session based authentication between, for example, a user device (i.e., such as a personal computer (PC), Internet appliance, laptop computer, smart card, radio telephone, or any other suitable device) and external system, such as a Web service on the Internet, or to processes within the same device. Cryptographic engines are often used to provide public key-based encryption, decryption, digital signing and signature verification as known in the art, and in such systems public and private key pairs are periodically generated and allow a user to digitally sign information, or decrypt information using private keys.

Session-based single factor authentication techniques are known wherein, for example, a first unit, such as a user device, is asked by a server which may contain, for example, credit card accounts, bank accounts or any other secure information, for the user to enter a user ID and a password to send so that the server can trust the user device. However, some such systems can be vulnerable to attack. For example, an attacker that maliciously obtains a user password can thereafter impersonate that user. Two factor authentication adds another level of security. For example, a server may return an authentication code, such as a random number generated by a random number generator in the server to the user device after the user entered the correct user ID and password. . The user device receives and digitally signs the received authentication code using a private signature key located on a smartcard that has been inserted into a smartcard reader at the user device, and returns the digitally signed authentication code over a same channel that was used to originally send the generated authentication code. However, deployment of such schemes is limited based at least on the monetary expense of supporting card readers at user devices.

Other two-factor authentication schemes are known, which do not require a hardware reader at the user device. For example, systems may use smart cards with display screens thereon in the following manner. The user is assigned a user ID and may select a personal identification number to be used as a password. A software routine running in a server such as a Web server or other suitable server, executes a similar routine executed by the smart card to generate a random number (authentication code) every few minutes. Although the smart card randomly generates a number every few minutes and the server randomly generates a random number every few minutes, these devices are typically not in communication with one another. These are two stand alone devices typically. When a user wishes to gain access to the server, the user uses the smart card by entering a PIN into the smart card. If the PIN is accepted, the smart card then displays the random number that it generates on the display device. At the same time the server generates a random number based on the same algorithm so that the numbers are

identical. The user then manually enters the displayed number in a keypad or other input device that is coupled to the server. The randomly generated number serves as a second level or second factor authentication code. However, because the two devices are not in communication and suitably synchronized, the server typically allows for a user to use a displayed random number that has previously been displayed as an acceptable number. In other words, there is a window during which time a server will accept more than one random number generated by the smart card. Accordingly, a problem can arise since an unscrupulous party may obtain the displayed number and still gain access to the system since the smart card and server are typically not in communication during a session, and multiple authentication codes can be used to gain access to the system.

Other two factor authentication techniques are known. For example, in some systems, a user is given a user ID and password and is e-mailed authentication information in an out of band communication, such that it is not sent during a session, to allow a user to enroll in a given system. However, the out of band authentication code could be intercepted and is not directly tied into a particular session.

Moreover, information security systems are being developed to allow a user to roam from one device to another. For example, a user profile that includes, for example, private keys such as private decryption keys and private signing keys along with user password information and other cryptographic keys, may be encrypted and stored in a server that is accessible by a user using a plurality of devices. The user profile is then sent to a user but only after an authentication procedure is carried out. Such authentication procedures may typically involve a user using a Web browser through which a user ID and password is entered. However, no other user-specific credentials are typically necessary. As a result, an unscrupulous party may gain access a user's private keys if they are able to obtain a user ID and password such as overlooking a user while a user is entering the information on a keyboard.

Accordingly, there exists a need for an improved authentication method and apparatus that overcomes one or more of the above deficiencies.

Brief Description Of The Drawings

FIG. 1 is a block diagram illustrating one example of an apparatus for providing user authentication in accordance with one embodiment of the invention;

FIG. 2 is a flow chart illustrating one example of a method for providing user authentication in accordance with one embodiment of the invention;

FIG. 3 is a block diagram illustrating a system for providing user authentication utilizing a wireless primary channel and back channel during a same session, in accordance with one embodiment of the invention;

FIG. 4 is a flow chart illustrating one example of a method for providing user authentication in accordance with one embodiment of the invention; and

Detailed Description Of The Preferred Embodiment

Briefly, a method and apparatus provides user authentication by communicating primary authentication information, such as user identification data and/or password data to an authentication unit via a primary channel such as over the Internet. An authentication code is generated by the authentication unit on a per session basis and is sent to the first device via an alternate or secondary channel during the session. The authentication unit determines which destination unit will receive the generated authentication code. As used herein, a unit may include multiple communication functions such as a telephone function, email function, pager function or any other suitable functions such that one Internet appliance, laptop computer or other unit may use one function to communicate on the primary channel, and another function on the alternate channel. If the determined destination unit is the same unit that originally sent the primary authentication information, the same unit returns the authentication code to the authentication unit, and the authentication unit then authenticates the user when the

returned authentication code matches the sent authentication code. Accordingly, a primary channel and an alternate channel is used during the same session to provide user authentication.

In another embodiment, an authentication unit determines which unit, other than the unit that originally sent the primary authentication information, will receive the generated authentication code. For example, where a user has a laptop computer being used as a first unit, and also has a pager or radiotelephone, as a third unit, that the user typically carries on his/her person, the authentication unit will use the primary authentication information that was sent by the first unit to determine which device to send the generated authentication code to based on, for example, the user ID sent as the primary authentication information. Accordingly, in one embodiment, an authentication database is maintained which contains per-user destination unit data, including, for example, a destination unit identifier such as a phone number of a radiotelephone, an IP address, a pager number, or any other suitable destination unit identifier which the authentication unit can use to contact and send the authentication code. A user, for example, that has a pager is sent the authentication code on their pager. The user may then enter the authentication code into the laptop computer to provide a second level of authentication by having the laptop then resend the generated authentication code back to the authentication unit via the primary channel used to originally send the primary authentication information, during the same session. Since the first unit, such as the laptop computer, and the second unit, such as a Web server, or any other unit that has access to an authentication unit, are in communication during the session, the authentication information that is also sent during the same session via an alternate channel is the only authentication code allowed to authenticate a user during a given session. Moreover, another device (a third unit), other than the device originally sending the primary authentication information, is sent the authentication code. A user must have access to the third unit and the first unit to complete the authentication process.

The secondary authentication information is typically an authentication code generated on a per session basis. This may include, for example, a pseudo random number or other suitable information. The authentication unit searches the database based on, for example, the sent user ID, to determine the telephone number of a radiotelephone or pager number associated with the user requesting authentication. The authentication code is sent to the designated unit via a wireless back channel during the session. The authenticator then determines whether the returned authentication code received from the wireless primary channel matches the sent authentication code that was sent on the wireless back channel to the third device.

FIG. 1 illustrates one example of a system for providing user authentication that employs a first unit 10 and a second unit 12. The first unit 10 may be, for example, an Internet appliance, radiotelephone, PDA, laptop computer or any other suitable device that provides primary authentication information, such as user ID information and/or a password, such as a personal identification number, to the second unit 12. The second unit 12 may be any suitable device including, but not limited to, a Web server, wireless network element, laptop computer, radiotelephone, Internet appliance, or any other suitable device. The system is shown, for purposes of illustration and not limitation, to be a system that employs the Internet. The first unit 10 and second unit 12 are operatively coupled via primary channel 14, such as a wired or wireless communication link. The first unit 10 may include, for example, a Web browser or any other suitable interface to allow the exchange of information with another device on the Internet. The second unit 12 is a Web server within the Internet 16, but may be any suitable device in any suitable system. The second unit 12, in this embodiment, also serves as an authentication unit to authenticate a user. As used herein, the word "user" includes a person and/or the first unit 10. The system also includes an authentication database 18 that is operatively coupled to the second unit 12 via a suitable link 20. The authentication database 18 contains destination unit data 22 on a per user basis. Accordingly, the authentication database 18 stores, for a plurality of users, on a per-user basis, a user ID 24, associated password or hashed password 26 (if used) and destination unit data 22.

The authentication database 18 may be populated based on a registration process carried out between a user device and the second unit 12. The second unit 12 also includes an authentication code generator 28 such as a random number generator to generate secondary authentication information that is sent back for use by the first unit 10.

During an authentication session, the second unit 12 sends a request 30 via primary channel 14 to the first unit 10 to request that the first unit send the user ID and password, where a password is used, to gain access to a desired system, software application or other process. During this session, the first unit 10 responds by sending the primary authentication information 32, namely, the user ID and password (if required). This may be provided, for example, by a person through an input device, such as a keypad. It may be a biometric input device, may be a hardware token, smart card or other suitable mechanism.

Referring also to FIG. 2, the operation of the system shown in FIG. 1 will be explained. During a registration process, a user registers with the authentication unit. The authentication unit creates a database entry for each user (or user device) that contains a user ID field, a password verification field (if used, or a one-way hash of the password) and a device address field. As shown in block 200, a method for providing user authentication includes sending, by the first unit 10, user identification data, such as the user ID on the primary channel 14 to the second device 12 which also serves, in this embodiment, as an authentication unit. Since the authentication database 18 is previously populated based on a registration process, the second unit 12 uses the received user identification data 32, to determine which destination unit will receive a generated authenticated code that is generated on an authentication session basis to be used as a second level of authentication to authenticate a user. For example, a user may have multiple destination units such as a radiotelephone, pager, or multiple PDAs to which the user wishes to have the authentication code sent. Also, the user may designate that the first unit 10 be the destination unit in which case the authentication code, also referred to

herein as the secondary authentication information, is sent to the first unit 10 as opposed to a unit other than the first unit. This is done by searching the authentication database 18 as indexed by the received user ID from the primary authentication information sent by the first unit 10. The second unit 12 matches the received user ID and if a password is used the associated hashed password, that was previously stored during the registration process to determine the appropriate destination unit identifier. The received password may be hashed and compared to the stored hash password. If there is a correlation, then the primary authentication is said to have succeeded, and the secondary authentication process may proceed using the destination unit identifier. One example of a destination unit identifier may be, for example, a telephone number associated with a given radiotelephone or other device that includes a radiotelephone, an IP address, that may be used, for example, to identify a pager or other device to which the authentication code is to be sent. Accordingly, as shown in block 202, the method includes using the user ID as an index to determine which destination unit will receive the authentication code generated by the authentication code generator 28 to authenticate a user. This is done based on the destination address 22 (from the device address field). As shown in block 204, the method includes sending the authentication code generated by the authentication code generator 28, such as a random number, or a derivation of the authentication code, during the same session to the determined destination unit that was determined based on the user ID and the destination address 22. In this embodiment, the destination unit is the first unit 10. As such, the destination unit address 22 may be an e-mail address or other suitable destination to which the second unit 12 will send the secondary authentication information, namely the generated authentication code. The authentication code that was generated by device 2 is sent during the same session via an alternate channel 34, such as a different time slot, frequency, Walsh code, IP address, telephone number or any distinguishing channel mechanism.

A shown in block 206, the method includes returning the received authentication code that was sent via the back channel, to the second unit, as shown by resent secondary authentication information 36. The authentication code may be suitably encrypted or

hashed or any other suitable representation may be sent back to the second unit 12. As shown in block 208, the method includes authenticating, by the second unit 12, the user (or user device) when the return authentication code or the resent secondary authentication information 36 matches the sent authentication code that was sent via the back channel 34. For example, the second unit 12 may store the generated authentication code from the authentication code generator 28 during the session and compare the resent authentication code 36 to the stored authentication code. If they match, the user is authenticated. As shown in block 210, the method includes waiting for a next session to authenticate the same or another user.

In a preferred embodiment, the first device 10 includes a cryptographic engine that provides requisite components of a public key infrastructure to allow the digital signing and verification of data as well as the encryption and decryption of information. Likewise, the second unit 12 includes one or more corresponding cryptographic engines that allow for digitally signing verification of digital signatures, encryption/decryption of information, or any other suitable operations as necessary. The above operations may be carried out by one or more processing units under software control. Alternatively, integrated circuits may also provide the requisite operations. Accordingly, the apparatus of FIGs. 1 and 2 may be implemented via hardware, software, or any other suitable combination thereof.

The second unit 12 sends the authentication code generated by the authentication code generator 28 to the determined destination unit based on the stored per-user destination unit identifier 22. Each user may have more than one destination unit address if, for example, a user has a pager, cell phone, or Internet appliance and may designate by a priority factor, which of the destination unit addresses is used as the primary address. Accordingly, if a person carries with them numerous devices, one device is the highest priority device and is first used to receive the secondary authentication information. The second unit 12 may then wait for the resent secondary authentication information 36 to be received within a defined period of time. If the resent authentication code is not received,

another or same authentication code may be sent to the next device of the next priority level as defined by the destination unit address after some predetermined amount of time has elapsed.

The method may also include receiving user input in response to the second unit sending the authentication code. For example, where the authentication code is sent via the alternate channel to the first device, the first device uses a graphic user interface to allow the user to input the authentication code and as such may activate a GUI button which then causes the authentication information to be resent back to the second device. Accordingly, the second device may wait to return the authentication code to the authentication unit 12 until receipt of the user input (e.g., entry of the authentication code).

In an alternative embodiment, the method may include, prior to returning the authentication code to the authentication unit, having the first unit digitally sign the received authentication code using a public key cryptographic engine prior to resending it back to the second unit. Digitally signing the received authentication code received via the back channel produces a digitally signed authentication code. Where the authentication code as resent is digitally signed, the second unit 12 verifies the digitally signed authentication code as part of the authenticating process by, for example, using conventional public key infrastructure techniques, as known in the art, to verify digital signatures.

Referring to FIGs. 3 and 4, an alternative embodiment is shown wherein the destination unit, other than the first unit, is used to receive generated authentication code. In addition, this embodiment shows a wireless communication system, such as a cellular Groupe Mobile Speciale (GSM) type system that employs, for example, a short messaging service (SMS) that provides, for example, text messaging via an alternate channel.

FIG. 3 illustrates a first unit 300, a second unit 302, an authenticator or authentication unit 304, the authentication database 18 and a third unit 306. In this embodiment, the authentication unit 304 is shown as being separate from the second unit 302. However, the authentication unit may be part of the second unit 302 which may be a Web server, wireless network element, or any other suitable device (as was shown in FIG. 1). The user 308, in this embodiment, may be, for example, a person. The first unit 300 and the second unit 302 are wireless devices that communicate over a primary wireless channel 310. The third unit 306 is also a wireless device, such as a pager or cell phone that communicates with the second unit 302 over a wireless back channel 312, such as an SMS channel.

The first unit 300 includes a primary channel controller, for example, a TCP/IP protocol stack used to communicate over the Internet to the second unit 302. The third unit 306 is preferably the personal property of the user 308, not a public device. As with the embodiment of FIGs1-2, the user 308, in a prior registration step, provides the destination unit identifier for each destination unit. In this example, one destination unit, namely the third unit 306, has been designated by a destination unit identifier 22. This identifier provides sufficient information in order to allow the third unit 306 to be communicated to from the second unit 302. This information is stored in the authentication database 18 and is available to the second unit 302, for example, through the authentication unit 304. The operation is similar to that previously described with reference to FIGs. 1 and 2, except in this embodiment, the generated authentication code as generated by the authentication code generator 28 in the second unit or in the authentication unit, is sent via a wireless alternate channel 312 to a unit other than the first unit 300. The authentication code is then provided to the user 308 via an audible or visual display associated with the third unit. The user through the user interface on the first unit, then inputs the authentication code into the first unit. The authentication code is then resent by the first unit to the second unit via the primary channel 310. The second unit 302 passes the resent authentication code to the authentication unit 304 where the authentication unit 304 compares the resent authentication code with the authentication

code that was sent to the third unit 306. If they match, the user (i.e. first unit) is granted access.

Also during the registration process, other users, such as user 2 also register with the authentication unit. As such, the authentication data base 18 includes user ID data 24, destination unit identifiers 22 and other authentication information such as whether a password is necessary for a plurality of users. In this example, user 2 has an authentication requirement that a password be used in addition to user ID 24. Accordingly, the authentication unit 304 uses the user identification data to determine, for example, which destination unit, other than the first unit 300, will receive authentication code generated on an authentication session basis, via the alternate channel 312 to be used to authenticate the user. If the user ID is for user 2, the authentication unit will inform the second unit 302 of the pager address associated with user 2 indicating the destination unit ID for user 2. Accordingly, user 2's pager will be sent the generated authentication code. If the user ID is the user ID for user 1, the destination unit identifier is an SMS address such as a short message service address used, for example, in a GSM cellular system. Accordingly, a radiotelephone unit associated with user 1 is contacted via an SMS channel during the session and is provided the authentication code via the back channel 312.

FIG. 4 illustrates one example for providing user authentication that may be implemented, for example, via the system shown in FIG. 3. However, it will be recognized that the disclosed methods herein can be carried out using any suitable structures and units and that the order of the steps may also be varied, if desired. In the above embodiments, a user wishes to access a resource controlled, for example, by the second unit via the first unit. Authentication is improved through the use of the alternate channel, through which authentication information is sent to a third device with a known address. The authentication information, such as the authentication code, is fed back through the primary channel to the second device thereby augmenting the authentication.

The user must have access to the third device and the primary authentication information entered at the first device in order to complete the authentication.

The first unit includes a plurality of software routines. One routine may be configured as a user input handler that accepts user input through a GUI interface or other suitable interface and provides output to the user in the form of a display or audio signal. Another software routine serves as an authentication controller that coordinates the relaying of information between the primary controller and the user input handler. Another software routine serves as the primary channel controller such as a TCP/IP protocol stack used to communicate over the Internet to the second unit. The primary channel controller maintains two way communication with another entity such as the second unit 302. Accordingly, the user input handler can be the conventional I/O capabilities of an Internet appliance or a laptop through a Web browser. The authentication controller may be a process or applet managing communication between the user input handler and any other components for the purposes of authenticating to the desired resource and may therefore interface, for example, with a cryptographic engine. The primary channel controller may be, for example, the TCP/IP protocol stack used to communicate over the Internet, or any other suitable communication controller and listened by may be for example a radio frequency transceiver to allow all of communications with the second unit. The second device as mentioned above, may be, for example, a Web server. The third device may be, for example, a paging device, PDA, or any other device that can provide visual or audible output to communicate the authentication code received from the second unit.

Referring again to FIG. 4, a user 308 may use the first unit 300 to contact the second unit 302 via primary wireless channel 310 wherein the second unit 302 has access-controlled resources requiring authentication. The second unit 302 sends a primary authentication information request to the first unit to prompt the user to enter primary authentication information. The user enters a user ID to identify the user to the second unit 302 and sends the user ID back over the primary wireless channel. This is

shown, for example, in steps 400 and 402. The second unit 302 contacts the authenticator 304 via a suitable communication link or bus, and passes the sent primary authentication information, namely the sent user ID, so that the authentication unit can determine if the user is listed in the authentication database 18. Accordingly, as shown in block 404, the method includes determining, based on a received user ID, which destination unit, other than the first unit 300, will receive an authentication code via the wireless back channel 312. The authentication code serves as secondary authentication information generated on an authentication session basis that is communicated via the wireless back channel to be used to authenticate the user. If the received user ID is listed in the database, the authentication unit retrieves the authentication record associated with the user. For example, this may include, for example, a user ID, SMS address, and other authentication information.

For example, if the user 308 has a GSM radiotelephone as the third unit 306, accessible via short messaging service, no other authentication data may be necessary. However, if the user has a pager, the pager network may require the entry of a password in addition to a user ID as part of the primary authentication information. The user in addition to entering the user ID, also enters a password that may be hashed by the first unit prior to communication to the second unit.

As shown in block 406, the method includes generating the authentication code to send to the third device during the same session. This is done, for example, by the authenticating code generator 28. The second unit sends a message over the primary channel 310 to the first device alerting the authentication controller to expect an authentication token message or authentication code. This causes a prompt for the authentication code to be displayed on the first device. The second unit sends a randomly generated, but locally stored authentication token or code to the third device via the alternate channel. This is shown in block 408. The third unit receives the authentication code via the back channel and displays it or otherwise transforms it for use or entry by the user into the first device. Accordingly, as shown in block 410, the user obtains the

authentication code from the third unit and enters it into the first unit. The first unit returns the authentication code obtained as received by the third unit back to the second unit via the primary wireless channel as shown in block 412. The authenticator, as shown in block 414, authenticates the user using the returned authentication code that was sent via the primary channel with the authentication code sent via the back channel. If they correlate, the user is authenticated and proceeds to use the appropriate resources via the second unit 302. Accordingly, the method includes returning the authentication code on the wireless primary channel to the authentication unit during the same session. The authenticator will authenticate the user when the returned authentication code received from the wireless primary channel, matches the sent authentication code that was sent on the wireless back channel. The authentication code generator 28 generates the authentication code on a per authentication session basis and the second unit sends the authentication code on a per authentication basis after it is generated. The authentication unit maintains per user destination unit data including the destination unit identifier per user such as a telephone number IP address or any other suitable data in the authentication database. The primary authentication information, such as the user ID, as sent from the first unit, is used to determine which destination unit will receive the authentication code generated by the authentication code generator 309. The authentication code is then sent to the defined destination unit as defined by the device address in the database associated with the user ID.

As noted in the previous embodiment, the first unit may also include a cryptographic engine that allows the first unit to digitally sign information. Accordingly, the method may include, prior to returning the authentication code to the authentication unit, the first unit digitally signing the authentication code to be returned, to produce a digitally signed authentication code. The authentication unit 304 then can subsequently verify the digitally signed authentication code as part of authenticating the user. If the authentication of the digital signature does not work, access is denied since it implies that a rogue party attempted to digitally sign a recovered authentication code with an improper digital signature.

It will be recognized that if desired, a suitable transformation may be applied to the authentication code. For example, a hash function may be used, so long as the transformation is expected by device 2 (as is the case with the authentication code being signed as stated above).

The above operations may be implemented by one or more processing devices that execute instructions stored in a storage medium. A storage medium may include, for example, one or more remotely accessible database via the Internet, a hard drive, RAM, ROM, CD ROMs, diskettes, or any other suitable storage medium containing executable instructions that when executed by one or more processors causes the one or more processors to carry out one or more of the above operations. For example, the storage medium may contain executable instructions that cause the authentication unit to receive, from the first unit, user identification data, that causes, for example, a processor associated with an authentication unit to use the user identification data to determine which destination unit, other than the first unit, will receive an authentication code to be used to authenticate the user. The storage medium may contain executable instructions that when executed by one or more processors causes one or more processors associated with authentication unit or other unit to send the authentication code to the determined destination unit based on the user identification data and to subsequently receive a returned authentication code back after sending the authentication code and authenticate the user, based on the returned authentication code when the returned authentication code matches the sent authentication code.

Accordingly, the above methods and apparatus allow differing levels of authentication. Moreover, an alternate channel is used during the session to provide authentication information in addition to user ID and/or a password to provide multi-factor authentication. In addition, sending the authentication code to a third unit that is owned by the user, improves the authentication process since only the user owns the third device and since the access cannot be granted without the party having access to both the

first unit and the first unit. Other advantages will be recognized by those of ordinary skill in the art.

It should be understood that the implementation of other variations and modifications of the invention in its various aspects will be apparent to those of ordinary skill in the art, and that the invention is not limited by the specific embodiments described. For example, although an embodiment has been described that uses a password as the example of the primary authentication mechanism it will be recognized that any primary authentication mechanism (as known in the art) as being used, e.g. biometric, such as voice recognition, or digital signature, given that the primary device contains a private signature key. Also, the database for the primary authentication information (e.g. password) may be different than the database for the destination unit data. The preferred embodiment should include them in the same database, but it may also be desirable to separate their storage. It is therefore contemplated to cover by the present invention, any and all modifications, variations, or equivalents that fall within the spirit and scope of the basic underlying principles disclosed and claimed herein.